UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/707,061	11/06/2000	Erno Zalka	4925-65	5796

7590 08/03/2004

Michael C Stuart Esq
Cohen Pontani Lieberman & Pavane
551 Fifth Avenue
Suite 1210
New York, NY 10176

EXAMINER	
PHAN, TRI H	

ART UNIT	PAPER NUMBER
2661	6

DATE MAILED: 08/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/707,061	ZALKA, ERNO	
	Examiner	Art Unit	
	Tri H. Phan	2661	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment/Arguments

1. This Office Action is in response to the Response/Amendment filed on May 06th, 2004. Claims 1-13 are now pending in the application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Miloslavsky** (U.S.6,418,146) in view of **Fuh et al.** (U.S.6,463,474).

- In regard to claim 1, **Miloslavsky** discloses in Figs. 1-4 and in the respective portions of the specification about the wireless access protocol service provider 'WAP-SP' ("*WAN gateway*"), e.g. enhanced proxy server, providing access to Internet data for WAP-enabled appliances enhanced with software, for facilitating telephony calls via wireless network ("*wireless telephone network*") in communicating with Web sites, e.g. Web servers ("*wide-area network servers*"), through the WAP-SP (For example see Fig. 1; Abstract); wherein the WAP device ("*mobile terminal*") must log in to the WAPSP via the authentication process ("*not*

previously logged in to the server"; For example see Figs. 3-4; col. 13, lines 11-15; col. 11, lines 60-65) and where the user's profile data is stored in the repository and forwarded to the web server ("*storing the information and forwarding to the server*"; For example see col. 13, lines 16-20, 64-67; col. 10, lines 4-12). Once authenticated, the WAP device may access services ("*previously logged in to the server*"), where the profile data is retrieved from the data repository for sending with the call to the web server ("*retrieving the stored login information and forwarding to the server*"; For example see Figs. 3-4; col. 13, lines 16-20, 64-67; col. 10, lines 4-12; col. 11, line 66 through col. 12, line 5). **Miloslavsky** does disclose about the authentication method and the login process, but fails to specifically disclose the step of method of "*determining whether*" the user has already or not yet logged in to the server. However, such implementation is known in the art.

For example, **Fuh** discloses in Figs 2-4 and 7A-B and in the respective portions of the specification about the method and firewall router ("*WAN gateway*") that provide network access control and locally authenticate the client to reduce network traffic to the authentication server, by comparing information identifying the client to the authentication cache information stored in the network device (For example see Abstract); wherein the firewall router with the authentication caches, through the use of Authentication proxy and filtering mechanism, determines whether the user is already or not yet authenticated ("*determining whether the user has already or not yet logged in to the server*"). If the user is not yet authenticated ("*not previously logged in to the server*"; See details in Fig. 7A, steps 708, 710 and Fig. 7B), the login form (See Fig. 5A) is provided to the user and the received login information is sent to the AAA server for performing authentication and authorization services, stored in the authentication

caches and sent to the target server ("*storing the information and forwarding to the server*"); and if the user is already authenticated ("*previously logged in to the server*"; See details in Fig. 7A, steps 708, 710 and 712), the user profile is stored and retrieved in the form of proxy-access list, and sent to the target server ("*retrieving the stored login information and forwarding to the server*") as disclosed in col. 9, line 1 through col. 15, line 55.

Thus it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the invention as taught by **Fuh**, by implementing the firewall's authentication process with the use of authentication caches, Authentication proxy and filtering mechanism into the authentication process of the WAP-SP, i.e. the enhanced proxy server, as taught by **Miloslavsky,** with the motivation being to improve the ability to provide network access control and locally authenticate the client in reducing network traffic to the authentication server.

- Regarding claims 2, 4-6, 8 and 11-13, **Miloslavsky** further discloses about the WAN is Internet (For example see Fig. 1; col. 5, lines 14-22), the login information comprises the username and password (For example see col. 9, lines 64-67), user is identified according to the telephone number (For example see col. 6, lines 1-7; col. 8, lines 4-16; wherein the user is identified according to his/her cell phone or fixed wireless telephone) and the server is identified according to its uniform resource locator 'URL' (For example see col. 5, lines 23-50; wherein the server is identified according to its URL through the server web page, where the user connects to the web page server via the network navigation software, i.e. WEB browser (For example see col. 5, lines 23-50).

- In regard to claims 3 and 9-10, **Miloslavsky** further discloses about the means for updating the request data coordinating with any additional data requirements during an ongoing call ("*modifying the login information by the user and forwarding to the gateway*"; For example see col. 12, lines 49-59; wherein various interaction paths of communication between WAP users and communication center, i.e. as disclose in details of WAP II and III in connection with WAP-SP, with additional profile data and routing options. It is also obvious that the user can modify the user name and password for different login process for different server connections, e.g. web page servers, via the network navigation software, i.e. WEB browser) and where the modification is stored in the caches ("*storing the modified information*") for authentication with the corresponding situations.

- Regarding claim 7, **Miloslavsky** discloses in Figs. 1-4 and in the respective portions of the specification about the wireless access protocol service provider 'WAP-SP' ("*WAN gateway*"), e.g. enhanced proxy server, providing access to Internet data for WAP-enabled appliances enhanced with software, for facilitating telephony calls via wireless network ("*wireless telephone network*") in communicating with Web sites, e.g. Web servers ("*wide-area network servers*"), through the WAP-SP (For example see Fig. 1; Abstract); wherein the data repository ("*data store*") stores the user data information for authentication process (For example see col. 7, lines 26-34; col. 8, lines 17-27), wherein the WAP device ("*mobile terminal*") must log in to the WAPSP via the authentication process ("*not previously logged in to the server*"; For example see Figs. 3-4; col. 13, lines 11-15; col. 11, lines 60-65) and where the user's profile data

is stored in the repository and forwarded to the web server ("*storing the information and forwarding to the server*"; For example see col. 13, lines 16-20, 64-67; col. 10, lines 4-12). Once authenticated, the WAP device may access services ("*previously logged in to the server*"), where the profile data is retrieved from the data repository for sending with the call to the web server ("*retrieving the stored login information and forwarding to the server*"; For example see Figs. 3-4; col. 13, lines 16-20, 64-67; col. 10, lines 4-12; col. 11, line 66 through col. 12, line 5). **Miloslavsky** does disclose about the authentication method and the login process, but fails to specifically disclose the step of method of "*determining whether*" the user has already or not yet logged in to the server. However, such implementation is known in the art.

For example, **Fuh** discloses in Figs 2-4 and 7A-B and in the respective portions of the specification about the method and firewall router ("*WAN gateway*") that provide network access control and locally authenticate the client to reduce network traffic to the authentication server, by comparing information identifying the client to the authentication cache information stored in the network device (For example see Abstract); wherein the firewall router with the authentication caches, through the use of Authentication proxy and filtering mechanism, determines whether the user is already or not yet authenticated ("*determining whether the user has already or not yet logged in to the server*" for the "*first logic*"). If the user is not yet authenticated ("*not previously logged in to the server*" for the "*second logic*"; See details in Fig. 7A, steps 708, 710 and Fig. 7B), the login form (See Fig. 5A) is provided to the user and the received login information is sent to the AAA server for performing authentication and authorization services, stored in the authentication caches and sent to the target server ("*storing the information and forwarding to the server*" for the "*fourth logic*"; and if the user is already

authenticated ("*previously logged in to the server*" for the "*third logic*"; See details in Fig. 7A, steps 708, 710 and712), the user profile is stored and retrieved in the form of proxy-access list, and sent to the target server ("*retrieving the stored login information and forwarding to the server*" for the "*fourth logic*") as disclosed in col. 9, line 1 through col. 15, line 55.

Thus it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to combine the invention as taught by Fuh, by implementing the firewall's authentication process with the use of authentication caches, Authentication proxy and filtering mechanism into the authentication process of the WAP-SP, i.e. the enhanced proxy server, as taught by Miloslavsky, with the motivation being to improve the ability to provide network access control and locally authenticate the client in reducing network traffic to the authentication server.

Response to Arguments

4. Applicant's arguments filed on May 06th, 2004 have been fully considered but they are not persuasive.

In regard to claims 1 and 7, Applicant argues that the combination of **Miloslavsky** and **Fuh** fails to disclose the method for "*storing the user name and password in the database and retrieving for the login*". Examiner respectfully disagrees. In response to Applicant's argument that the combination of references fails to show a certain feature of Applicant's invention, it is noted that the feature upon which Applicant relies (i.e. "*storing the user name and password in the auto login database, retrieving for the login and forwarding it to the server*") is not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations

from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir.1993).

More than that, **Miloslavsky** does discloses about the wireless access protocol service provider 'WAP-SP' ("*WAN gateway*"), e.g. enhanced proxy server as disclosed in col. 5, lines 51-57, providing access to Internet data for WAP-enabled appliances enhanced with software, for facilitating telephony calls via wireless network ("*wireless telephone network*") in communicating with Web sites, e.g. Web servers 'WS' ("*wide-area network servers*"; For example see Figs. 1-2), through the WAP-SP; wherein the WAP device ("*mobile terminal*") must log in with user name and password pair ("*user name and password*") to the WAP-SP for the authentication process ("*retrieving for the login*"; For example see Figs. 2 and 4; col. 9, line 64 through col. 10, line 3; col. 11, lines 60-65) for communicating with WSs 19 or 21 ("*particular server*"; For example see Figs. 1-2), and where the user profiles ("*particular user login information*", e.g. personal information, as disclosed in col. 7, lines 26-34) are stored in the data repository ("*storing the login information in the database*"; For example see col. 8, lines 17-27; col. 3, lines 38-41) and forwarded the profile data to the web server 'WS' ("*forwarding the login information to the server*"; For example see col. 10, lines 4-12 and 49-53).

Fuh also discloses about the method and firewall router ("*WAN gateway*") that provide network access control and locally authenticate the client to reduce network traffic to the authentication server, by comparing information identifying the client to the authentication cache information stored in the network device (For example see Abstract); wherein the firewall router with the authentication caches, through the use of Authentication proxy and filtering mechanism, determines whether the user is already or not yet authenticated ("*determining whether the user*

has already or not yet logged in to the server"). If the user is not yet authenticated ("*not previously logged in to the server*"; See details in Fig. 7A, steps 708, 710 and Fig. 7B), the login form (See Fig. 5A) is provided to the user and the received login information is sent to the AAA server for performing authentication and authorization services, stored in the authentication caches and sent to the target server ("*storing the information and forwarding to the server*"); and if the user is already authenticated ("*previously logged in to the server*"; See details in Fig. 7A, steps 708, 710 and 712), the user profile is stored and retrieved in the form of proxy-access list, and sent to the target server ("*retrieving the stored login information and forwarding to the server*") as disclosed in col. 9, line 1 through col. 15, line 55.

Therefore, Examiner concludes that the combination of **Miloslavsky** and **Fuh** teaches the arguable features.

Claims 2-6 and 8-13 are rejected as in Part 3 above of this Office action and by virtue of their dependence from claims 1 and 7.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Jin et al. (U.S.6,643,782), **Short et al.** (U.S.6,636,894), **Isomichi et al.** (U.S.2001/0000358) and **Skemer** (U.S.2001/0044893) are all cited to show devices and methods for improving the authentication in the telecommunication architectures, which are considered pertinent to the claimed invention.

6. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tri H. Phan, whose telephone number is (703) 305-7444. The examiner can normally be reached on M-F (8:00-4:30).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Douglas W. Olms can be reached on (703) 305-4703.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

or faxed to:

(703) 872-9314

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Sixth Floor.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Technology Center 2600 Customer Service Office, whose telephone number is (703) 305-3900.

Tri H. Phan
July 15, 2004